Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Using SignalFlow in Splunk Observability Cloud

CODE:	LENGTH:	PRICE:
SPL_USFSOC	16 Hours (2 days)	Request Price

Description

This 2-day (virtual days) course is targeted towards SREs, ITOps, and DevOps Engineers who are responsible for implementing and maintaining an observability solution for infrastructure and application monitoring. In this advanced technical course, you will learn to use SignalFlow – the analytics language used in Splunk Observability Cloud. SignalFlow is a programming language used to define Charts, Navigators and Detectors, and for more complicated data manipulation.
Use SignalFlow to develop visualizations and detectors that are more specific and reusable than what is possible using the user interface alone. You will create functions to analyze data and to incorporate elements from the Observability Cloud code library. The content covered in this course is essential to managing Observability Cloud resources as code using the REST API, Terraform or another contentas-code solution.
Learn the concepts and apply the knowledge through demonstrations, discussions and hands-on activities.
Note: *Much of the content in this course was previously covered in the retired course "Automation and the REST and SignalFlow APIs"*

Objectives

Module 1 – Writing Your First SignalFlow Program

- Identify where SignalFlow is used in Splunk Observability Cloud
- Create plots using SignalFlow instead of the Plot Builder
- Query streaming data
- Add filters to streaming data queries
- Combine filters with and, or, not

Module 2 – Working with Data Streams in Splunk Observability Cloud

- Describe the fundamentals of Data Stream objects
- Use aggregation functions to analyze streaming data
- Apply transformations to streaming data
- Change resolutions, rollups, and extrapolation policies when querying streaming data

Module 3 – Stream aggregations, transformations, and calculations

- Use combining operators on streams
- Operate on data streams with missing data
- Use the map() method to modify or exclude values in a stream
- Describe variable assignment in SignalFlow
- Differentiate between SignalFlow functions and methods
- Describe and use SignalFlow functions that have equivalent methods

Module 4 – Detecting and Alerting in SignalFlow

- Use the detect() function to monitor a stream

- Use comparisons to create Boolean streams
- Create constant streams and use them appropriately
- Specify different "on" and "off" conditions for a detect block
- Identify durations of an occurrence in streaming data
- Compare streams using different thresholds for different MTSs
- Create alerts rules that align with detectors

Module 5 – Advanced Detecting and Stream Manipulation

- Work with properties and dimensions in SignalFlow
- Compare values using multiple thresholds and a default
- Use built-in library functions
- Use conditional, list, and other Python-like functionality
- Write reusable functions in SignalFlow

Module 6 – The SignalFlow REST API

- Explain the SignalFlow APIs available and common use cases
- Execute a SignalFlow program using the HTTP API
- Describe the data format returned by the HTTP API
- Explain how Terraform is used to manage Infrastructure Monitoring resources in Splunk Observability Cloud
- Create detectors and alert rules using the REST API

Audience

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Prerequisites

- Visualizing and Alerting Splunk Observability Cloud
- Experience working with programming languages such as Python (preferred), JavaScript, or Go.

Note: If you have not worked extensively with Splunk Observability Cloud you should take another course first before continuing with this one.

Programme

- Writing your first SignalFlow program
- Working with Data Streams in Splunk Observability Cloud
- Stream aggregations, transformations, and calculations
- Detecting and alerting in SignalFlow
- Advanced detecting and stream manipulation
- The SignalFlow REST API

Test and Certification

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

Further Information

Course Format
Instructor-led lecture with labs, delivered via live virtual classroom.

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.